

IN THE CLAIMS

Claims 1-9, 12, 13 and 15-32 are pending. Claims 10, 11, and 14 were previously canceled; and claims 24, 25, 26, 27, 29 and 31 are amended herein.

1 1. (Previously Presented) A fingerprint recognizing display system comprising:
2 a monitor having a screen and a front cover surrounding said screen;
3 a fingerprint recognizing module included with said monitor, said fingerprint
4 recognizing module including a fingerprint image recognizing unit disposed on a surface
5 of said front cover, wherein a user desiring access to said fingerprint recognizing display
6 system touches said fingerprint image recognizing unit; and
7 a computer main body including a fingerprint data base and a fingerprint verifying
8 unit, wherein said fingerprint verifying unit compares fingerprint data transmitted from
9 said fingerprint recognizing module to registered fingerprint data stored in said
10 fingerprint data base and permits said user access to programs stored in said fingerprint
11 recognizing display system when it is determined that the fingerprint of said user matches
12 fingerprint data stored in said fingerprint data base, said computer main body comprising:
13 a kernel of an operating system of said computer main body for
14 determining whether said fingerprint data base has been established in said
15 computer main body; and
16 said kernel recognizing that said fingerprint recognizing display system has
17 been activated and performing a fingerprint registration routine when it is
18 determined that said fingerprint data base has not been established, and

19 determining whether said monitor is a fingerprint recognizing monitor when it is
20 determined that said fingerprint data base has been established.

1 2. (Original) The fingerprint recognizing display system as set forth in claim 1,
2 wherein said fingerprint image recognizing unit is integrally formed with a power switch
3 disposed on the surface of said front cover.

1 3. (Original) The fingerprint recognizing display system as set forth in claim 1,
2 wherein said fingerprint recognizing module also includes:

3 a converter converting analog fingerprint data input from the fingerprint image
4 recognizing unit to digital fingerprint data, and

5 a first communication unit transmitting the digital fingerprint data to a second
6 communication unit in the computer main body.

1 4. (Original) The fingerprint recognizing display system as set forth in claim 1,
2 wherein said monitor includes a microprocessor communicating with a video card in said
3 computer main body.

1 5. (Original) The fingerprint recognizing display system as set forth in claim 4,
2 wherein said fingerprint recognizing module also includes:

3 a converter converting analog fingerprint data input from the fingerprint image
4 recognizing unit to digital fingerprint data, and

5 said microprocessor transmits the digital fingerprint data to a communication unit
6 in the computer main body.

1 6. (Previously Presented) The fingerprint recognizing display system as set forth
2 in claim 1, wherein said fingerprint verifying unit includes:

3 a decoding unit for decoding the registered fingerprint data read from said
4 fingerprint data base;

5 an encoding unit for encoding fingerprint data for storage into said fingerprint data
6 base;

7 a distinctive feature detecting unit for detecting a distinctive feature of a
8 fingerprint corresponding to the fingerprint data transmitted from said monitor;

9 a fingerprint matching/recording unit for receiving decoded fingerprint data from
10 said decoding unit and also for providing fingerprint data to said encoding unit, said
11 fingerprint matching/recording unit comparing decoded fingerprint data received from
12 said decoding unit to said distinctive feature received from said distinctive feature
13 detecting unit and also for outputting said distinctive feature received from said
14 distinctive feature detecting unit to said encoding unit to be stored as the registered
15 fingerprint data in said fingerprint data base; and

16 a recognizing unit outputting a "pass" signal or a "fail" signal in response to a
17 comparison result output from said fingerprint matching/recording unit.

1 7. (Previously Presented) The fingerprint recognizing display system as set forth

in claim 3, wherein said fingerprint verifying unit includes:

a decoding unit for decoding the registered fingerprint data read from said fingerprint data base;

an encoding unit for encoding fingerprint data for storage into said fingerprint data base;

a distinctive feature detecting unit for detecting a distinctive feature of a fingerprint corresponding to the fingerprint data transmitted from said first communication unit to said second communication unit;

a fingerprint matching/recording unit for receiving decoded fingerprint data from said decoding unit and also for providing fingerprint data to said encoding unit, said fingerprint matching/recording unit comparing decoded fingerprint data received from said decoding unit to said distinctive feature received from said distinctive feature detecting unit and also for outputting said distinctive feature received from said distinctive feature detecting unit to said encoding unit to be stored as the registered fingerprint data in said fingerprint data base; and

a recognizing unit outputting a "pass" signal or a "fail" signal in response to a comparison result output from said fingerprint matching/recording unit.

8. (Previously Presented) The fingerprint recognizing display system as set forth in claim 5, wherein said fingerprint verifying unit includes:

a decoding unit for decoding the registered fingerprint data read from said fingerprint data base;

5 an encoding unit for encoding fingerprint data for storage into said fingerprint data
6 base;

7 a distinctive feature detecting unit for detecting a distinctive feature of a
8 fingerprint corresponding to the fingerprint data transmitted from said microprocessor to
9 said communication unit;

10 a fingerprint matching/recording unit for receiving decoded fingerprint data from
11 said decoding unit and also for providing fingerprint data to said encoding unit, said
12 fingerprint matching/recording unit comparing decoded fingerprint data received from
13 said decoding unit to said distinctive feature received from said distinctive feature
14 detecting unit and also for outputting said distinctive feature received from said
15 distinctive feature detecting unit to said encoding unit to be stored as the registered
16 fingerprint data in said fingerprint data base; and

17 a recognizing unit outputting a "pass" signal or a "fail" signal in response to a
18 comparison result output from said fingerprint matching/recording unit.

1 9. (Original) The fingerprint recognizing display system as set forth in claim 1,
2 wherein said monitor comprises a cathode ray tube display apparatus or a liquid crystal
3 display apparatus.

1 10. (Canceled)

1 11. (Canceled)

1 12. (Previously Presented) A method of recognizing a fingerprint to enable a user
2 to operate a computer system including a monitor and a computer main body, said method
3 being embodied in an operating system kernel mode and comprising the steps of:

4 determining whether a fingerprint data base has been established in said computer
5 main body;

6 performing a fingerprint registration routine when it is determined that said
7 fingerprint data base has not been established,

8 determining whether said monitor is a fingerprint recognizing monitor when it is
9 determined that said fingerprint data base has been established;

10 detecting a fingerprint of the user when said user touches a portion of a front cover
11 surrounding a display screen of said monitor of said computer system;

12 transmitting fingerprint data corresponding to said fingerprint of said user, when
13 detected, from said monitor to said computer main body of said computer system;

14 comparing the fingerprint data transmitted from said monitor to registered
15 fingerprint data output from said fingerprint data base, when said fingerprint data base
16 has been established in said computer main body; and

17 enabling said computer system to be operated by said user when said comparing
18 step indicates that there is a match between the fingerprint data transmitted from said
19 monitor and the registered fingerprint data output from said fingerprint data base, or
20 disabling said computer system to prevent operation by said user when said comparing
21 step indicates that there is not a match between the fingerprint data transmitted from said

22 monitor and the registered fingerprint data output from said fingerprint data base.

1 13. (Previously Presented) The method as set forth in claim 12, further comprising
2 steps of:

3 determining that said monitor is operating in an abnormal status and preventing
4 said computer system from being operated when it is determined that said monitor is not a
5 fingerprint recognizing monitor, or performing said step of detecting a fingerprint when it
6 is determined that said monitor is a fingerprint recognizing monitor.

1 14. (Canceled)

1 15. (Original) The method as set forth in claim 13, further comprising steps of:
2 determining whether a keyboard or a mouse of said computer system is operated by
3 said user during operation of a screen protection routine of said computer system; and
4 continuing to run a screen saver program when it is determined that neither said
5 keyboard nor said mouse have been operated, or performing said step of determining
6 whether said monitor is a fingerprint recognizing monitor when it is determined that one
7 of said keyboard or said mouse have been operated.

1 16. (Original) The method as set forth in claim 15, further comprising a step of
2 ending said screen protection routine when said comparing step indicates that there is a
3 match between the fingerprint data transmitted from said monitor and the registered

4 fingerprint data output from said fingerprint data base, and then performing said step of
5 enabling said computer system to be operated by said user.

1 17. (Original) The method as set forth in claim 12, wherein said comparing step
2 includes steps of:

3 checking said fingerprint data transmitted from said monitor and detecting
4 distinctive features thereof;

5 determining whether the detected distinctive features are of good quality; and
6 outputting an error message when it is determined that the detected distinctive
7 features are not of good quality and returning to said step of detecting a fingerprint of the
8 user, or performing said comparing step when it is determined that the detected
9 distinctive features are of good quality.

1 18. (Previously Presented) The method as set forth in claim 13, further comprising
2 steps of:

3 determining whether a file stored in said computer system is enabled to be encoded
4 or decoded during operation of a file encoding/decoding routine of said computer system;

5 outputting an message indicating said file can not be encoded or decoded when it
6 is determined said file is not enabled to be encoded or decoded;

7 performing said step of determining whether said monitor is a fingerprint
8 recognizing monitor when it is determined said file is enabled to be encoded or decoded;
9 and

10 permitting said user to encode or decode said file when said comparing step
11 indicates that there is a match between the fingerprint data transmitted from said monitor
12 and the registered fingerprint data output from said fingerprint data base.

1 19. (Previously Presented) The method as set forth in claim 12, wherein said
2 fingerprint registration routine comprises the steps of:

3 detecting a fingerprint of a manager when said manager touches the portion of the
4 front cover of said monitor of said computer system;

5 transmitting fingerprint data corresponding to said fingerprint of said manager,
6 when detected, from said monitor to said computer main body of said computer system;

7 comparing the fingerprint data transmitted from said monitor to registered
8 fingerprint data output from a fingerprint data base included in said computer main body;
9 and

10 permitting said manager to operate a fingerprint managing and registering program
11 when said comparing step indicates that there is a match between the fingerprint data
12 transmitted from said monitor and the registered fingerprint data output from said
13 fingerprint data base, or disabling said computer system to prevent operation by said
14 manager when said comparing step indicates that there is not a match between the
15 fingerprint data transmitted from said monitor and the registered fingerprint data output
16 from said fingerprint data base.

1 20. (Previously Presented) A method of recognizing a fingerprint to enable a user

2 to operate a computer system including a monitor and a computer main body, said method
3 being embodied in a kernel of an operating system of said computer main body and
4 comprising the steps of:

5 determining whether a fingerprint data base has been established in said computer
6 main body;

7 performing a fingerprint registration routine when it is determined that said
8 fingerprint data base has not been established; and

9 determining whether said monitor is a fingerprint recognizing monitor when it is
10 determined that said fingerprint data base has been established.

1 21. (Previously Presented) The method as set forth in claim 20, wherein said
2 fingerprint registration routine comprises the steps of:

3 detecting a fingerprint of a manager when said manager touches a portion of a
4 front cover of said monitor of said computer system;

5 transmitting fingerprint data corresponding to said fingerprint of said manager,
6 when detected, from said monitor to said computer main body of said computer system;

7 comparing the fingerprint data transmitted from said monitor to registered
8 fingerprint data output from a fingerprint data base included in said computer main body;
9 and

10 permitting said manager to operate a fingerprint managing and registering program
11 when said comparing step indicates that there is a match between the fingerprint data
12 transmitted from said monitor and the registered fingerprint data output from said

13 fingerprint data base, or disabling said computer system to prevent operation by said
14 manager when said comparing step indicates that there is not a match between the
15 fingerprint data transmitted from said monitor and the registered fingerprint data output
16 from said fingerprint data base.

1 22. (Previously Presented) The method as set forth in claim 20, further comprising
2 steps of:

3 detecting a fingerprint of the user when said user touches a portion of a front cover
4 surrounding a display screen of said monitor of said computer system;

5 transmitting fingerprint data corresponding to said fingerprint of said user, when
6 detected, from said monitor to said computer main body of said computer system;

7 comparing the fingerprint data transmitted from said monitor to registered
8 fingerprint data output from said fingerprint data base, when said fingerprint data base
9 has been established in said computer main body; and

10 enabling said computer system to be operated by said user when said comparing
11 step indicates that there is a match between the fingerprint data transmitted from said
12 monitor and the registered fingerprint data output from said fingerprint data base, or
13 disabling said computer system to prevent operation by said user when said comparing
14 step indicates that there is not a match between the fingerprint data transmitted from said
15 monitor and the registered fingerprint data output from said fingerprint data base.

1 23. (Previously Presented) The method as set forth in claim 20, further comprising

2 steps of:

3 determining that said monitor is operating in an abnormal status and preventing
4 said computer system from being operated when it is determined that said monitor is not a
5 fingerprint recognizing monitor, or performing said step of detecting a fingerprint when it
6 is determined that said monitor is a fingerprint recognizing monitor.

1 24. (Currently Amended) An information device recognizing a fingerprint, the
2 information device comprising:

3 a fingerprint data base storing registered fingerprint data;

4 a fingerprint verifying unit comparing fingerprint data transmitted from an
5 external device to the fingerprint verifying unit; and

6 a kernel of an operating system of the information device permitting access to a
7 program stored in the information device when the fingerprint verifying unit determines
8 that transmitted fingerprint data match the registered fingerprint data, wherein the kernel
9 determines whether the fingerprint data base has been established in the information
10 device, recognizes that the external device and the information device have been
11 activated and performs a fingerprint registration routine when it is determined that the
12 fingerprint data base has not been established.

1 25. (Currently Amended) An information device recognizing a fingerprint, the
2 information device comprising:

3 a fingerprint data base storing registered fingerprint data;

4 a kernel of an operating system of the information device; and

5 a fingerprint verifying unit comparing fingerprint data transmitted from an
6 external device to the fingerprint verifying unit and controlling the kernel to execute a
7 program stored in the information device when the fingerprint verifying unit determines
8 that the transmitted fingerprint data match the registered fingerprint data, wherein the
9 kernel determines whether the fingerprint data base has been established in the
10 information device, recognizes that the external device and the information device have
11 been activated and performs a fingerprint registration routine when it is determined that
12 the fingerprint data base has not been established.

1 26. (Currently Amended) An information device recognizing a fingerprint, the
2 information device comprising:

3 a fingerprint data base storing registered fingerprint data;

4 a fingerprint verifying unit comparing fingerprint data transmitted from an
5 external device to the fingerprint verifying unit; and

6 a kernel of an operating system of the information device permitting access to
7 electronic commerce through the information device when the fingerprint verifying
8 device determines that the transmitted fingerprint data match the registered fingerprint
9 data, wherein the kernel determines whether the fingerprint data base has been
10 established in the information device, recognizes that the external device and the
11 information device have been activated and performs a fingerprint registration routine
12 when it is determined that the fingerprint data base has not been established.

1 27. (Currently Amended) The information device according to claim 24, wherein
2 the kernel determines whether ~~the fingerprint data base has been established in the~~
3 ~~information device, recognizes that the external device and the information device have~~
4 ~~been activated and performs a fingerprint registration routine when it is determined that~~
5 ~~the fingerprint data base has not been established, and determined whether the external~~
6 device is a fingerprint recognizing device when it is determined that the fingerprint data
7 base has ~~[[not]]~~ been established.

1 28. (Previously Presented) The information device according to claim 27,
2 wherein the external device comprises a monitor including a fingerprint recognizing
3 module including a fingerprint image recognizing unit and transmitting the fingerprint
4 data recognized by the fingerprint image recognizing unit to the information device.

1 29. (Currently Amended) The information device according to claim 25, wherein
2 the kernel determines whether ~~the fingerprint data base has been established in the~~
3 ~~information device, recognizes that the external device and the information device have~~
4 ~~been activated and performs a fingerprint registration routine when it is determined that~~
5 ~~the fingerprint data base has not been established, and determined whether the external~~
6 device is a fingerprint recognizing device when it is determined that the fingerprint data
7 base has ~~[[not]]~~ been established.

1 30. (Previously Presented) The information device according to claim 29,
2 wherein the external device comprises a monitor including a fingerprint recognizing
3 module including a fingerprint image recognizing unit and transmitting the fingerprint
4 data recognized by the fingerprint image recognizing unit to the information device.

1 31. (Currently Amended) The information device according to claim 26, wherein
2 the kernel determines whether ~~the fingerprint data base has been established in the~~
3 ~~information device, recognizes that the external device and the information device have~~
4 ~~been activated and performs a fingerprint registration routine when it is determined that~~
5 ~~the fingerprint data base has not been established, and determined whether the external~~
6 device is a fingerprint recognizing device when it is determined that the fingerprint data
7 base has ~~[[not]]~~ been established.

1 32. (Previously Presented) The information device according to claim 31,
2 wherein the external device comprises a monitor including a fingerprint recognizing
3 module including a fingerprint image recognizing unit and transmitting the fingerprint
4 data recognized by the fingerprint image recognizing unit to the information device.